

ICCRTS 2014

Agile and Adaptive IT Ecosystem, Results, Outlook , and Recommendations

Authors

- Harvey Reed, Multi-Party Engineering, MITRE, hreed@mitre.org
- John Nankervis, Mission Partner Environment, CIV Joint Staff J6, john.t.nankervis.civ@mail.mil
- LtCol Jordon Cochran (USAF), OUSD(AT&L), jordon.t.cochran.mil@mail.mil
- Rajeev Parekh, US BICES Chief Engineer, MITRE, rparekh@mitre.org
- Fred Stein, Col. U.S. Army (ret), Network Centric Warfare, MITRE, fstein@mitre.org

POC

- Harvey Reed, hreed@mitre.org

Contributing

- Robert (Pat) Benito, Multi-Party Engineering, MITRE, rbenito@mitre.org
- Chris Magrin, DISA PEO-C2C Chief Engineer, MITRE, cmagrin@mitre.org
- Diane Hanf, Multi-Party Engineering, MITRE, dhanf@mitre.org
- Michelle Casagni, Multi-Party Engineering, MITRE, mcasagni@mitre.org

Report Documentation Page		Form Approved OMB No. 0704-0188
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.		
1. REPORT DATE JUN 2014	2. REPORT TYPE	3. DATES COVERED 00-00-2014 to 00-00-2014
4. TITLE AND SUBTITLE Agile and Adaptive IT Ecosystem, Results, Outlook , and Recommendations		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER	
	5e. TASK NUMBER	
	5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) MITRE,202 Burlington Road,Bedford,MA,01730		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited		
13. SUPPLEMENTARY NOTES Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 16-19 June, 2014 in Alexandria, VA. U.S. Government or Federal Rights License		
14. ABSTRACT The missions of the U.S. military require great operational adaptability and depend critically on obtaining information support via networks. The information technology (IT) that enables these networks typically takes the form of single, large, ?releasable to US only? systems that are difficult to adapt during a mission. This will present a growing problem in the expected operating environment for U.S. forces, which will feature coalition actions in which all partners operate at the same security and releasability levels and share information and data as equals. In a 2012 ICCRTS paper1 the authors proposed that the military adopt an ?Agile and Adaptive Ecosystem (AAE)? approach to IT development. The system engineering process for AAE uses Multi-Party Engineering, featuring Shared Agreements that capture roles and responsibilities when components such as widgets, gadgets, or plug-ins are independently developed, delivered, and assembled into capabilities. The present paper builds on those findings and reports the results of efforts to create an AAE throughout the Department of Defense. It describes the challenges posed by aspects of the component lifecycle for business, information assurance, licensing for assembling capabilities, and federated markets over a variety of technology. It then examines the relevance of the AAE to networked environments such as the Joint Information Environment Mission Partner Environment Tier 1, which represents persistent information exchange among specific sets of partner nations, and Tier 2, which features Joining, Membership, and Exiting Instructions for federating ?partner nation contributed IT? into a Combined/Joint Task Force (C/JTF) ?mission network.? The C/JTF federated mission network represents a larger grained analogy to Shared Agreements, federated markets, and assembled capabilities. Finally, the paper presents initial recommendations on guidance, policy. and material development for AAE.		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 36	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Abstract

The missions of the U.S. military require great operational adaptability and depend critically on obtaining information support via networks. The information technology (IT) that enables these networks typically takes the form of single, large, “releasable to US only” systems that are difficult to adapt during a mission. This will present a growing problem in the expected operating environment for U.S. forces, which will feature coalition actions in which all partners operate at the same security and releasability levels and share information and data as equals.

In a 2012 ICCRTS paper¹ the authors proposed that the military adopt an “Agile and Adaptive Ecosystem (AAE)” approach to IT development. The system engineering process for AAE uses Multi-Party Engineering, featuring Shared Agreements that capture roles and responsibilities when components such as widgets, gadgets, or plug-ins are independently developed, delivered, and assembled into capabilities.

The present paper builds on those findings and reports the results of efforts to create an AAE throughout the Department of Defense. It describes the challenges posed by aspects of the component lifecycle for business, information assurance, licensing for assembling capabilities, and federated markets over a variety of technology. It then examines the relevance of the AAE to networked environments such as the Joint Information Environment Mission Partner Environment Tier 1, which represents persistent information exchange among specific sets of partner nations, and Tier 2, which features Joining, Membership, and Exiting Instructions for federating “partner nation contributed IT” into a Combined/Joint Task Force (C/JTF) “mission network.” The C/JTF federated mission network represents a larger grained analogy to Shared Agreements, federated markets, and assembled capabilities. Finally, the paper presents initial recommendations on guidance, policy, and material development for AAE.

¹ “Supporting Agile C2 with an Agile and Adaptive IT Ecosystem,” ICCRTS 2012, Reed, Benito, Collens, Stein: http://dodccrp.org/events/17th_icrts_2012/post_conference/papers/044.pdf

Vision: Assembling IT Capabilities

In the ICCRTS 2012 paper “Supporting Agile C2 with an Agile and Adaptive IT Ecosystem”² Reed, Benito, Collens, and Stein proposed an alternative to delivering standalone information technology (IT) systems within the U.S. Department of Defense (DoD): assembling IT capabilities from components offered in markets. These components would incorporate the latest commercial technology frameworks and be independently provided and upgraded. Over time, providing increasing numbers of components in markets and assembling IT capabilities from those components would create an Agile and Adaptive Ecosystem (AAE). AAEs have five key attributes:

1. Component providers employ agile development techniques to build components, which are subsequently hosted in markets. These techniques increase the probability that providers will build components with required functionality, and enable the providers to make user-requested modifications. Users can assemble larger capabilities from components hosted in markets as they need them, and re-assemble capabilities as components and mission needs change.
2. Federated markets unify the ecosystem. The DoD/IC space differs from the commercial space in that value is maximized by increasing the span over which markets are federated, not by limiting them.
3. Collaboration across all key participants is necessary to maintain a healthy AAE. For example, the acquisition and development communities require direct, high-quality user feedback to build or tailor the right components, while component certifiers must collaborate early and often with the development community regarding expectations for certification. This increases efficiency, and allows for quicker certification of components for operational use.
4. The AAE uses a modified version of the commercial pay-per-use business model to generate value. The customer pays only for the apps and services used, which creates monetary incentives for the DoD and IC development community to accommodate users’ needs. The incentives benefit government and military app developers and those who actively work with them.
5. The AAE operates through portfolios, not large programs of record. The AAE acquires small components via agile methods, and teams use portfolio management techniques to govern the markets. These teams decide what components and services to invest in based on feedback from customers.

The emerging systems engineering discipline of Multi-Party Engineering captures the tenets of using components offered in markets to assemble IT capabilities and build the AAE. The tenets of Multi-Party Engineering are:

² “Supporting Agile C2 with an Agile and Adaptive IT Ecosystem”, ICCRTS 2012, Reed, Benito, Collens, Stein: http://dodccrp.org/events/17th_icrts_2012/post_conference/papers/044.pdf

1. Provide small components that are later assembled into capabilities. This leads to a very beneficial decoupling of the early production of components from the late assembly of capabilities. The components are delivered in a short timeframe, and are versionable.
2. Certify components to Shared Agreements among participants. Shared Agreements capture assembly requirements (e.g., certification and accreditation [C&A], authorization, data, etc.), and components are certified as meeting the Shared Agreements. The agreements constrain usage to ensure compatibility, and can address security, accreditation, testing, data semantics, etc. Component developers can also be certified, attesting to their ability to provide components that conform to various Shared Agreements.
3. Offer certified components in markets. Shared Agreements capture assembly requirements (e.g., C&A, authorization, data, etc.), and components are certified as meeting the Shared Agreements as a prerequisite for components to be offered in markets. These markets are conceptually similar to markets in commercial smartphones, extended to accommodate many types of components. This decouples the provision of components from assembly of capabilities in terms of time, yet maintains integrity in the final assembly. The market governance assures Shared Agreements are versioned and current.
4. Assemble capabilities from the components offered in markets. Components are assembled into capabilities close to the time when the capability is initially needed; the capability can subsequently be adapted and tailored. Thanks to the Shared Agreements, less time is needed to assemble certified components into capabilities. Further, assembling reusable components avoids costs, and the resources saved can be applied to tailor the capability to the needs of different missions.
5. Solicit and respond to feedback from end users . Capabilities evolve as components are updated and new components are introduced on the basis of direct feedback from end users. The feedback is captured through end user engagement, made available to the component providers, and maintained in markets associated with the respective components that serve as repositories of knowledge regarding how components and Shared Agreements should be refined.

The Shared Agreements help all the stakeholders create a “trust bridge” among separate programs where none may exist because at present stakeholders align themselves by individual systems. A Shared Agreement may be a temporary construct that informs future institutional policy and/or guidance, or have a longer life if policy or guidance remain unchanged. This approach enables the DoD to take advantage of recent advances in commercial technology (e.g., open source, mobile, and cloud technology), with the tradeoff of requiring sufficient Shared Agreements to enable reuse of components among providers and consumers. Figure 1 illustrates the contrast between the current system-oriented approach for delivering IT capabilities and the emerging AAE approach.

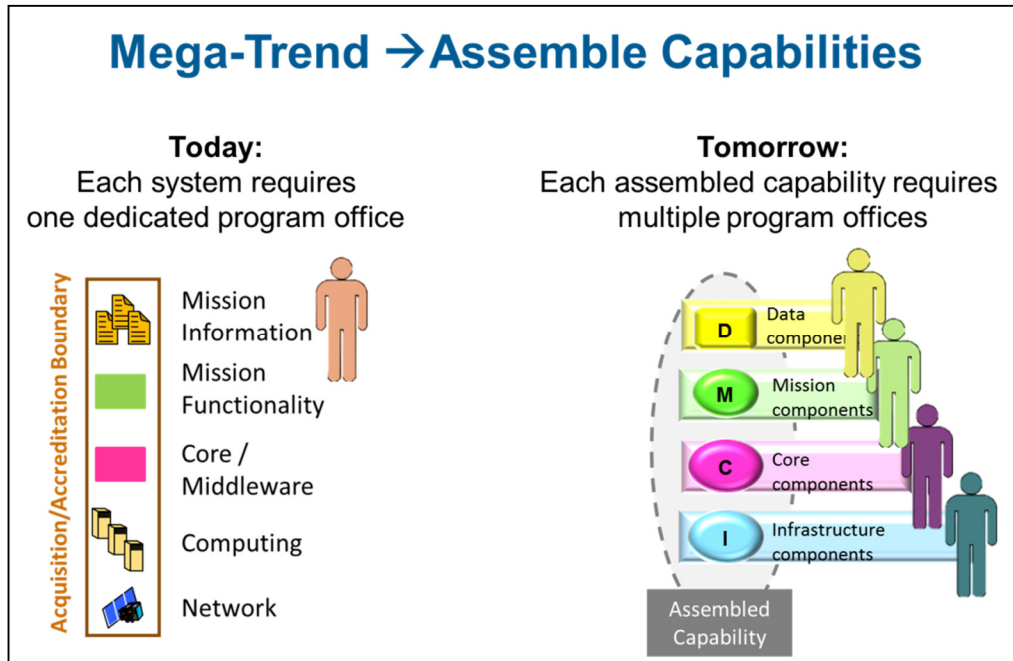


Figure 1. Multi-Party Engineering

In this paper, we examine initial results achieved by some DoD organizations that have applied Multi-Party Engineering and make recommendations for potential follow-on activities. We close by noting parallels between the use of Shared Agreements in Multi-Party Engineering and the use of Joining, Membership, and Exiting Instructions (JMEI) during the standup and operation of a Combined Joint Task Force (C/JTF), as typified in Mission Partner Environment Tier 2.

Results

Various direct efforts across multiple communities have started to practice Multi-Party Engineering by providing components (new, harvested, etc.), assembling IT capabilities, hosting, etc. Most are in progress, and some are complete, as noted. Table 1 shows these efforts, grouped by the type of activity they represent. Please note these are examples, and not intended to be a comprehensive listing.

Table 1. Summary of Efforts

Type of Effort	Description	Activity Level	Examples
IT Capability	Use a variety of mission and core infrastructure components to assemble an IT capability	Significant	<ul style="list-style-type: none"> Joint Logistics Enterprise Data Sharing (JLEDs),

			<p>complete</p> <ul style="list-style-type: none"> • C-130 Electronic Flight Bag,³ in progress
New components; components harvested by deconstructing legacy components	Employ methods that range from community-wide data calls to identify new and/or potentially reusable services, to harvesting as a result of legacy deconstruction. Some components are traded across joint and/or family of systems organization boundaries.	Significant	<ul style="list-style-type: none"> • Global Command and Control System – Joint (GCCS-J) and ACF (Agile Client Framework),⁴ complete • Defense Intelligence Information Environment-Framework (DI2E-F),⁵ in progress • Theater Battle Management Core System-Unit Level (TBMCS-UL), Command and Control Information Systems / Command and Control Air Operations Suite (C2IS/AOS),⁶ in progress
Hosting, platform	Engage in efforts ranging from classic hosting to cloud migration	Significant	<ul style="list-style-type: none"> • Global Combat Support System – Air Force (GCSS-AF), complete • Federal Risk and Authorization Management Program (FEDRAMP),⁷ complete • CIO Cloud Strategy,⁸ complete • Defense Information

³ <http://www.forbes.com/sites/matthewstibbe/2013/05/30/u-s-air-force-will-save-50m-with-ipad-electronic-flight-bags/>

⁴ <http://netbeans.dzone.com/news/war-fighter-netbeans-platform>

⁵ http://www.afei.org/events/4A07/Documents/1-DI2E%20Brochure%20ISA_10APR13.pdf

⁶ <https://it-2014.itdashboard.gov/investment/exhibit300/pdf/007-000001911>

⁷ <http://cloud.cio.gov/fedramp>

⁸

<http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf>

			Systems Agency (DISA) Cloud Broker, ⁹ in progress
Mobile	Effort to use smartphones and other mobile devices	Very significant	<ul style="list-style-type: none"> • CIO Mobility Strategy,¹⁰ complete • National Geospatial-Intelligence Agency (NGA) Geospatial Intelligence (GEOINT) App Store,¹¹ in progress • DoD Mobility,¹² in progress • General Services Administration (GSA) Managed Mobility,¹³ in progress
Markets and federation	Broad need to trade components across Title 10 and other organization boundaries.	Emerging	<ul style="list-style-type: none"> • Combatant Commands (COCOMs) and Services, in progress
Component cybersecurity reciprocity	Ability to trade components across designated Authorizing Official (AO) boundaries	Emerging	<ul style="list-style-type: none"> • DoD Widget Working Group (WG), in progress

We draw a key distinction between providing and using components within one organization and trading components across organizations, since the value of reuse only becomes manifest when programs can trade components across large organizational distances. The ability to trade components depends on the reciprocity of cybersecurity assessments; otherwise the receiving organization must perform new cybersecurity assessments for every component, thereby losing much of the value of trading components.

The JLEDS example illustrates the goal of assembling IT capabilities as needed and a variety of challenges that organizations will meet as they practice Multi-Party Engineering more broadly (discussed further below). Given the current drawdown, the logistics community needs better visibility of transportation options in order to move supplies and equipment out of Afghanistan expeditiously and cost effectively.

⁹ <http://www.disa.mil/Services/DoD-Cloud-Broker>

¹⁰ <http://www.defense.gov/news/dodmobilitystrategy.pdf>

¹¹ <https://apps.nga.mil/>

¹² <http://www.disa.mil/Services/Enterprise-Services/Mobility>

¹³ http://www.gsa.gov/portal/content/159903?utm_source=FAS&utm_medium=print-radio&utm_term=managedmobility&utm_campaign=shortcuts

Within approximately one year JLEDS combined existing DISA enterprise services with appropriate data sources and a new Ozone Widget Framework (OWF) widget to create an IT capability tailored for this activity. Authorizing operation of this required agreement among multiple AOs.

The component cybersecurity reciprocity effort now in progress seeks ways to use the recently released DoDI 8510.01 Risk Management Framework (RMF) policy to express component-level cybersecurity assessments. DoD efforts could then trade the assessments along with the components across large organizational distances without having to repeat the assessment each time a trade occurs.

The DoD Widget WG¹⁴ engages with direct efforts to understand what both the provider and receiver of a component require so they can produce or reuse an assessment, respectively. The group provides this detailed knowledge to policy makers in the form of feedback and ongoing dialogue. The DoD Widget WG does not write policy or dictate actions to the direct efforts and their associated AOs; it simply facilitates the creation of a Shared Agreement among the participating direct efforts in order to establish a common context when creating examples for policy groups that illustrate program needs. The Shared Agreement would include:

- Nominal lifecycle for a widget – the parties need to agree on a common lifecycle with steps for providing and using a widget, such that the provider and receiver can agree on the point in the lifecycle at which the component, including the cybersecurity assessment, is handed off from one organization to another.”
- Definition of the roles and responsibilities, in generic terms, for the various steps in the nominal lifecycle. Each participating organization can map the steps to their descriptions of specific billets in its organization chart. Such generic descriptions would promote clarity regarding specific roles / responsibilities when handing off components.
- Templates for component-level cybersecurity assessment – agreed among the direct efforts. Each of the direct efforts can then “fill in” the templates to create worked examples, allowing respective provider/receiver pairs to agree on how to trade assessments together with the components.

The Shared Agreement resulting from this effort must remain in force long enough to accommodate sufficient feedback loops, while policy groups can be informed by the worked examples of direct effort assessments.

Maturity Scale

As the direct efforts mentioned in Table 1 gain experience with various activities involved in practicing Multi-Party Engineering, the DoD must consider how to measure that experience. Multi-Party Engineering does not have an official “maturity scale” in the sense of Capability Maturity Model

¹⁴ https://intellipedia.intelink.gov/wiki/DoD_Widget_Working_Group

Integration (CMMI).¹⁵ In this section we examine the ability of programs to practice the tenets of Multi-Party Engineering, noting that maturity remains very uneven across direct efforts (e.g., acquisition programs such as the AF's C2IS/AOS), community efforts (e.g., DI2E-F), and enterprise efforts (e.g., the recent publication and promulgation of DoDI 8510.01).

Some activities, such as component “vetting” and testing for mobile apps produced by a single organization for its own use, reveal high levels of activity and experience. Organizations have less experience in activities such as certifying components, which involves establishing the desired features and capabilities of a component and then performing tests to determine whether or not the component meets the standards. If the component passes the tests, a certifying authority or test authority attests that the component has certain characteristics and can supply the test data to prove it. This must be a community activity, with strong governance. Individual organizations have little incentive to expend the extra effort required to characterize and certify a component strictly for their own use, except for very basic purposes such as characterizing a mobile app in order to choose the best acquisition processes for either a Government off-the-Shelf (GOTS) or commercial off-the-shelf (COTS) capability.

The list below notes the observed state of maturity in DoD programs of the five tenets of Multi-Party Engineering outlined in the previous section. The maturity rating is based on experiential observations by the authors and discussions within the various communities of practice regarding the ability to support a component lifecycle.¹⁶ This encompasses not only providing components and assembling capabilities, but also obtaining feedback that prompts subsequent updates to one or more components and dependent assembled capabilities. The descriptions draw some terminology from the newly released DoDI 8510.01;¹⁷ for example, they use “AO” (Authorizing Official) as the term that supersedes the earlier term DAA (Designated Approving Authority).¹⁸ Each tenet leads to the next.

1. *Provide Small Components.* Both the Agile Client and Ozone Web Framework marketplaces demonstrate that program offices can build and/or acquire a component for their own use. However, even in this simple case, once the component is available for use, using that component even within the same program office in its own previously accredited baselines presents significant challenges. They include component vetting, and incrementally adding a component to a baseline (assembly).
2. *Certify Components to Shared Agreements.* Ongoing activities within DI2E-F¹⁹ aim to understand what it means for the community to agree (certify) that a service (component) is suitable for

¹⁵ <http://www.sei.cmu.edu/cmmi/>

¹⁶ In a future paper we intend to formalize the definition of maturity and engage direct efforts in a structured assessment.

¹⁷ http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

¹⁸ See the DAU Glossary for a complete set of terms: http://www.dau.mil/pubscats/pubscats/13th_edition_glossary.pdf

¹⁹ <https://intellipedia.intelink.gov/wiki/DI2E-F>

reuse, at least within the certifying community. Activities within DISA²⁰ and NSA²¹ are seeking approaches to standardize vetting of mobile apps.

3. *Offer Components in Markets.* Some markets are relatively mature, such as the NGA GEOINT app store;²² other markets are only beginning to develop. In some tactical cases, the DoD does not use markets in order to prevent changes to component configuration in the field. Markets and their associated and federated governances provide an agreement structure regarding which components can be used for assembling IT capabilities. For example, the government office assembling a capability needs to be assured of the legal, business, cyber security, and other compliance of a component, and have a government structure for managing dependencies. Use of markets requires cybersecurity reciprocity of components.
4. *Assemble Capabilities.* The government has built a few types of assemblies at various levels of maturity. For example:
 - Hosting – GCSS-AF²³ presents a very mature example of full-service hosting²⁴ of a variety of components, from data services to Enterprise Resource Planning (ERP) modules. It can host small vetted components in 10 days on average. This works well in a community setting where the applicable AOs have established Shared Agreements to add the components incrementally to the shared hosting infrastructure, such as in Air Force combat support. Most communities do not have this level of agreement.
 - Dedicated function – Some early examples of dedicated function-assembled capabilities (e.g., JLEDS) are appearing. Since no established guidance exists for such assemblies, all of the related AOs must participate in the process for approving the assembly.
 - Dashboard – Typical of the OWF Widget²⁵ paradigm, a server hosts several instances of web apps that are visualized as tiles in a browser for the purpose of organizing data for the user. This mode is gaining traction, but still encounters IA challenges, and requires AO Shared Agreements to trade and use components.
 - Mobile – Rapid assembly of mobile apps is gaining popularity. The DoD CIO and DISA are establishing strategies, but need to overcome cybersecurity reciprocity challenges to trade and use components.
5. *Solicit and respond to feedback from users.* MPE grows an AAE over time, at many scale levels²⁶ by using feedback from end users as input to the requirements and governance of markets. No

²⁰ <http://www.disa.mil/Services/Enterprise-Services/Mobility/Request-Mobile-App>

²¹ <http://www.amarcedu.org/wp-content/uploads/2014/03/CAS.pdf>

²² <https://apps.nga.mil/>

²³ <https://itdashboard.gov/investment?buscid=62>

²⁴ http://www.dodsbir.net/sitis/view_pdf.asp?id=AF141-206_Ref_4_GCSSAF_Intro_1.15.14.pdf

²⁵ <https://www.owfgoss.org/>

²⁶ <http://necsi.edu/research/multiscale/>

central planning takes place; however, developers receive feedback from users²⁷ through local and community centers of federated governance. Some feedback loops are emerging at the direct, community, and enterprise levels. The feedback loops are ultimately the most important feature of the ecosystem, since without them the developers will not provide the right components and assemble the right capabilities. The shorter time to assembly makes feedback loops much more important than when the average time to deliver a system was 7.5 years. When the component cycle is 9 months, or even 3 months, accurate feedback is of paramount importance.

Challenges

The government must trade the unsolvable problem of drastically reducing the time²⁸ and cost of typical systems delivery²⁹ for the significant – but solvable – problems of providing components and assembling capabilities. However, the government faces challenges to advancing the maturity of enterprise, community, and direct Multi-Party Engineering efforts.

The first concerns ensuring cybersecurity within the context of the recent DoD Instruction (DoDI) 8510.01,³⁰ which directs programs to adopt the NIST RMF.³¹ In implementing 8510.01 the DoD should create sufficient Shared Agreements that various organizations can trade and use each other's components (a) without repeating component vetting assessment tests,³² and ideally also (b) having similar approaches to assessing risk and authorizing usage of a component. Programs should establish sufficient Shared Agreements on the lifecycle of components, assembly of capabilities using components with different pedigrees and intended uses, and associated roles and responsibilities, particularly for testing and assessing cybersecurity characteristics,³³ to forge agreements across Title 10 and other organizations.

²⁷ Users include functional end users, as well as all principals pertinent to the components and assembled capabilities, including testing, finance, legal, etc.

²⁸ NDAA 2010 sec. 804 calls for 6–18 month delivery of IT capability: <http://www.gpo.gov/fdsys/pkg/BILLS-111hr2647enr/pdf/BILLS-111hr2647enr.pdf>

²⁹ For example, the Software Engineering Institute (SEI) delivered an insightful report on aspects of system delivery that can be improved in the context of NDAA 2010 sec. 804, but the DoD is still constrained by standalone system timelines and sequences of events. With assembly of capabilities, the DoD can save time by reusing previously developed components, and quickly assemble IT capabilities by using Shared Agreements created in advance. The Shared Agreements may be in the form of policy or guidance that explicitly enables cooperation and coordination among multiple parties. SEI report: <http://www.sei.cmu.edu/reports/11sr015.pdf>

³⁰ http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

³¹ <http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training/index.html>

³² For example, an 8510.01 Product-level Security Assessment Report (SAR)

³³ For example, Common Weakness Enumeration (CWE), which characterize weaknesses in software only components: <https://cwe.mitre.org/>

Currently the RMF TAG³⁴ is responsible for the implementation of 8510.01 and is collaborating with various efforts to ensure appropriate implementation guidance is published in a timely fashion. The DoD Widget WG works with direct efforts and the RMF TAG to establish feedback loops and accelerate development of cybersecurity reciprocity.

A second challenge relates to creating a business model that enables repeatable and rapid acquisition of components and assembled capabilities. The business model must incentivize commercial developers to want to participate within the ecosystem. Acquiring components rather than systems runs counter to the present DoD acquisition culture, but still falls within established regulatory guidelines as published in the Federal Acquisition Regulation (FAR).³⁵ Numerous efforts across several agencies are exploring the new processes needed for acquiring COTS and GOTS components, particularly in the mobile app space. Early indications show that current processes can evolve in an orderly fashion to accommodate a variety of models.

Promoting market federation to enable trading of components via markets across Title 10 and other boundaries poses another challenge. Market federation will generate significant reuse benefits, primarily from a time-to-market perspective. At present the government is pursuing two main types of federation: a central market and a federated market. Currently DISA is charged with providing the central mobile app market for the DoD³⁶ (as noted, organizations such as NGA have their own app markets). DISA will not necessarily provide all the mobile apps, so DISA, other Title 10, and other organizations will need to establish sufficient federation agreements organizations that mobile apps can be provided from any approved organization and listed in the DISA mobile market. The market will maintain certain minimum standards (security, business, etc.). By contrast, the COCOMs are interested in federation as a means to interact not only with their Service military components, but also with the coalition information sharing environment.

The government must also build a community that facilitates highly matrixed sharing of practices and case studies across direct, community, and enterprise efforts. several communities already develop and share practices, and cooperate to maintain awareness, share developments, etc. Since the ecosystem has many scales, and efforts occur at the direct, community, and enterprise levels, the communities of practice are by necessity highly matrixed. These communities offer an opportunity for enterprise leadership to gather feedback and to “get the word out” on policy and guidance. Ultimately the government must capture Multi-Party Engineering practices and experience and incorporate them in case studies for schoolhouse education and training. Candidate schoolhouses include the Defense

³⁴ RMF TAG (Technical Advisory Group), see para 1.c. of 8510.01

³⁵ <http://www.acquisition.gov/far/>

³⁶ <http://www.disa.mil/Services/Enterprise-Services/Mobility/DoD-App-Store>

Acquisition University (DAU),³⁷ West Point,³⁸ U.S. Naval Academy (USNA)³⁹ and USNA Marines,⁴⁰ and the USAF Academy.⁴¹

Finally, the DoD must create an infrastructure that allows the DoD to maintain a baseline of platforms that host various types of components. A variety of component technologies can be hosted on either infrastructure platforms or user-facing platforms (or both). The challenges are synchronizing the development and maintenance of components and their hosting platforms outside the construct of a program delivering a functional standalone system. The DoD uses a number of server container technologies, including Java, .NET, OWF (servlet), OWF Joint Command and Control Common User Interface (JC2CUI) variant (servlet), Agile Client (NetBeans), and OSGI bundles (Karafe). DoD systems also use both the Android and iOS mobile operating systems. Each technology has a specific type of server baseline that must be maintained, plus most likely two previous versions for release compatibility purposes. The associated challenges involve maintenance of technology baselines outside the construct of a program delivering a functional standalone system. In addition, options exist at the community and enterprise levels to stand up centrally managed instances of servers for convenience and cost reduction purposes. However, this incurs additional challenges regarding funding: whether central or pay-per-use. Finally, each type of server baseline needs a Government Open Source Software (GOSS) structure similar to that already established for OWF (regular) and Agile Client. This governance vets requirements from stakeholders and allocates them to releases.

Outlook

The prospects for broadening and maturing the practice of Multi-Party Engineering seem positive. The committed early adopters engaged in the direct efforts noted above are both maturing the practice and engaging in communities of practice to accelerate universal adoption. Similarly, a number of early adopter leaders (DoD CIO, AT&L, Joint Staff, etc.) are advancing initiatives to pave the way for broad adoption in the near future.

Joint Information Environment (JIE)

Currently the bulk of direct, community, and enterprise efforts in Multi-Party Engineering are developed, deployed, and used in the context of the U.S. and regional and mobile networks that are evolving to the JIE. This already provides great advantages, but the full value of these components and assembled capabilities will be amplified once the capabilities are deployed as needed in operational and

³⁷ <http://www.dau.mil/default.aspx>

³⁸ <http://www.usma.edu/SitePages/Home.aspx>

³⁹ <http://www.usna.edu/homepage.php>

⁴⁰ <http://www.usna.edu/USMC/>

⁴¹ <http://www.usafa.af.mil/>

coalition mission networks (e.g., Mission Partner Environment Tier 2), in order for the warfighter and analyst to use these capabilities

The Multi-Party Engineering approach, together with the above recommendations, supports the primary objectives of the JIE. Pacific Command (PACOM), which is implementing JIE Increment 2, described its vision of JIE as follows:

Improved Mission Effectiveness / Operational Flexibility – Agile information systems that enable C2 for all [PACOM] missions and any set of [PACOM] partners including mobile, deployed units and individuals; across wide and diverse geography; resilient in disconnected, intermittent and low-bandwidth (DIL) network environments.

Increased Cyber Security – Robust information systems that provide the confidentiality, integrity, and availability needed to assure C2 for all [PACOM] missions and any set of PACOM partners.

IT Efficiencies / Joint Information Services – Interoperable information systems developed and implemented with maximum performance, reliability and extensibility at best value and minimum waste.⁴²

The Multi-Party Engineering approach supports PACOM's goals for JIE by shifting the paradigm of delivering IT capability from standalone systems to assembled capabilities. Assembled capabilities by definition will reuse existing infrastructure, platforms, and networks. The approach also advances cybersecurity by reusing tested and proven infrastructure, platforms, networks, and promotes IT efficiencies by discouraging duplication and providing components and updates.

At present, the unit of acquisition delivery is typically a complete system baseline. By contrast, Multi-Party Engineering enables programs to deliver fine-grained components as well as assembled IT capabilities, so the acquisition delivery can now be as small as a highly tailored mission component. Small units of delivery accelerate the time to field.

Multi-Party Engineering contributes to mission effectiveness by focusing component acquisition and upgrades on mission functionality rather than on reinventing supporting infrastructure. The unit of acquisition delivery now includes the mission-focused assembled capability and reuses shared infrastructure.

Assembled capabilities can be run in a variety of environments. Market federation supports using components in a variety of shared infrastructure areas, such as consolidated data centers,⁴³ and enables component discovery in a wide scale.

⁴² Randy Cieslak (Chief Information Officer, PACOM), "Reaching Coalition Partners through the Joint Information Environment (JIE): Background and Challenges," presented at Armed Forces Communications and Electronics Association (AFCEA), Tech Net Asia-Pacific (TNAP), 5 December 2013; <http://www.afcea.org/events/asiapacific/13/documents/JIE-Coalition-CIESLAK-131205Bv2.pdf> The presentation describes the current state of JIE and the intersection with the Mission Partner Environment (MPE).

Mission Partner Environment

The networks through which the United States and her partner nations cooperate to accomplish mutually agreed objectives, including sharing information, are collectively known as the Mission Partner Environment. The Mission Partner Environment could benefit significantly from Multi-Party Engineering and the resulting AAEs because:

1. The components, markets, and assembled IT capabilities are starting to add value in the JIE. The value will be fully realized once DoD programs can deploy assembled capabilities to operational networks, including the Mission Partner Environment. Currently programs are just starting to deploy assembled IT capabilities to operational networks. As this process continues, the AAE would grow, and could then span networks that support generating the force as well as the operational networks.
2. The agreement structure required for assembling IT capabilities resembles the agreement structure in Mission Partner Environment.

The set of networks that persist across events⁴⁴ for long-term collaboration are called Mission Partner Environment Tier 1, and include networks controlled under bi-lateral (United States plus one partner nation) or multi-lateral (United States plus multiple other partner nations) agreements. These networks and the associated standards (constituting a type of Shared Agreement) were created for political reasons and support treaties rather than individual events. The networks that enable collaboration with partner nations during an event are called Mission Partner Environment Tier 2. More precisely, the United States brings its Tier 2 national network extension and federates with network extensions from other partner nations to create a federated mission network, such as the Afghan Mission Network, that operates at a single mission-REL classification level. The network extensions are federated via physical boxes called Network Interface Points (NIPs), following guidelines for federation captured in Joining, Membership, and Exiting Instructions (JMEI) for that event, and are based on a JMEI template.

The JMEI presents an analogy to Shared Agreements because the United States maintains its JMEI template and coordinates the template with other partner nations. The JMEI is governed laterally; for example, a partner nation that disagrees with an aspect of a JMEI can seek to rally support for improvements, but obtains that support one country at a time, rather than working through a central governance entity.

⁴³ Core Data Center Reference Architecture:

<http://www.dodenterprisearchitecture.org/program/Documents/Chhibber%20CDC%20RA%20Conference@1330.pdf>

⁴⁴ The term “event” can refer to exercises, demonstrations, humanitarian assistance/disaster relief (HADR), wide area security, Major Combat Operations (MCO), etc.

Under the JMEI, the participating nations assemble IT capabilities for warfighters and analysts to use during events, both in the context of a C/JTF and other operational networks. Assembly occurs at the level of IT and of the operational network. The assembly involves four phases. The first consists of assembling the IT capability itself. Next, an event occurs, and the participating nations create a C/JTF (see below) to establish a federated mission network. Third, the participants populate the operational networks, including the federated mission network of the C/JTF, with the assembled IT capabilities. Fourth and finally, the participants substitute components of the assembled IT capability as necessary to tailor the capability to the particular needs of the mission. The resulting AAE would therefore span from the generate-the-force networks that support acquisition, test, training, and the like to the operational networks, maintaining the crucial properties of agility and adaptability across the networks (see Figure 2).

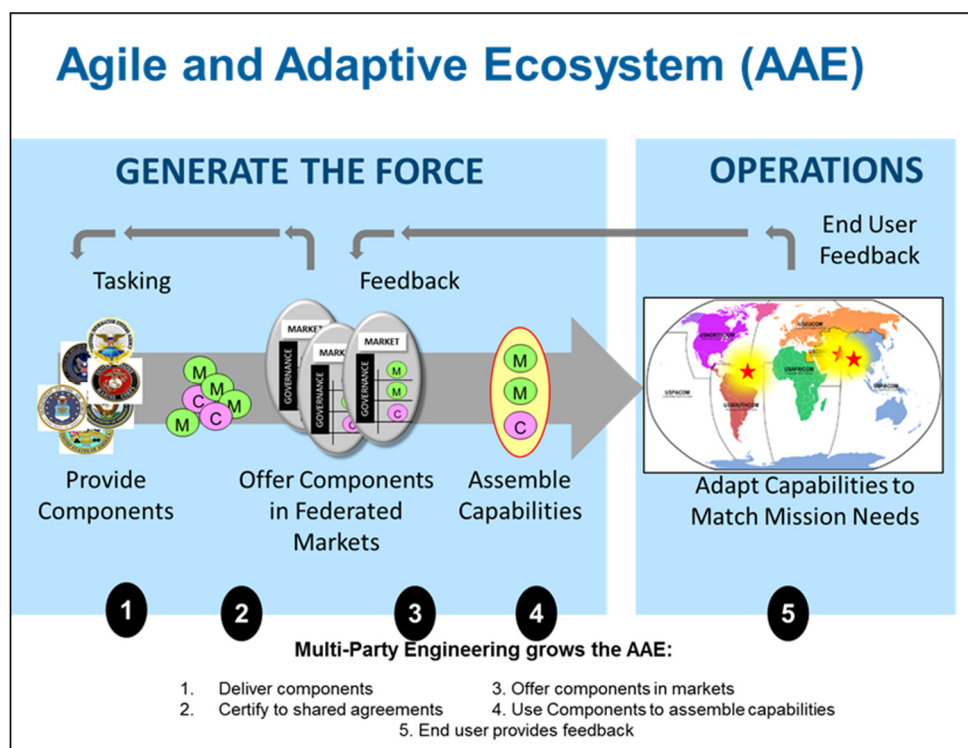


Figure 2. AAE Spans Generate the Force and Operational Networks

A C/JTF uses a federated mission network assembled when an event is declared, and after a task force is created and a commander chosen, by tailoring the JMEI for that event from a JMEI template. COMBINED ENDEAVOR 2013⁴⁵ showed that the countries that studied and followed the JMEI could federate quickly. Once the federated mission network exists, the C/JTF can assemble the military forces in the usual fashion. Within a C/JTF information sharing occurs openly and completely. If any partner nation, including the United States, must withhold information, that information must flow through country

⁴⁵ <https://www.youtube.com/watch?v=OeFaOGHyQMk>

networks outside the federated mission network of the C/JTF. Since the network operates at the mission-REL level, participating nations must put the appropriate information protection methods in place to move information into and out of the network, just as with any other movement of information across classification domains.

COMBINED ENDEAVOR illustrates how Shared Agreements for events could operate. The Shared Agreements beginning to be used in the AAE and Multi-Party Engineering activities share the lateral governance characteristics of JMEIs. Over the longer term some Shared Agreements might evolve to inform traditional top-down policy and guidance.

Changing Perspectives

The DoD is on the cusp of dramatic changes in how it responds to events: from applying “overwhelming force” and massive amounts of hardware against conventional adversaries to acting rapidly and adaptively against non-state actors. As the Capstone Concept for Joint Operations: Joint Force 2020 (CCJO 2020)⁴⁶ points out in the foreword, “In this concept, Joint Force elements, globally postured, combine quickly with each other and mission partners to integrate capabilities fluidly across domains, echelons, geographic boundaries, and organizational affiliates.”

The notion of assembly at multiple scales, as represented by Multi-Party Engineering and the AAE concept, supports the ability to combine quickly in support of the CCJO vision. Given the large number of cooperating parties that would act at multiple scale levels in the AAE, the structure of the Shared Agreements governing the various scale levels of assembly would be critical for success. The existing Shared Agreements for components, markets, and assembled IT capabilities are still immature and largely focused on component vetting. Shared Agreements that can enable component cybersecurity reciprocity would open the door for widespread trading of components, and more market and assembly Shared Agreements would appear. It is worth repeating that Shared Agreements would also foster trust and new behaviors. As the agreements inform institutional policy and guidance, the Shared Agreements can be replaced with more formal policy and guidance.

The scale levels of assembly, and the points in time in which they manifest themselves would lead to new forms of agility. For example, the requirements for providing components are based on past events. Components would be offered in a market in anticipation of future demand, and thus be available for use in an assembled IT capability as the need arises. When an event occurs, the C/JTF would populate the federated mission network with assembled IT capabilities that represent the best thinking from past events. During the event situations could arise that would prompt users to change how the assembled capabilities are used, or alter the assembled capability by substituting a component or even creating a new component, and so on. This would increase the “potential agility” of the C/JTF.⁴⁷ Mission needs

⁴⁶ http://www.dtic.mil/futurejointwarfare/concepts/ccjo_2012.pdf

⁴⁷ http://www.dodccrp.org/files/agility_advantage/Agility_Advantage_Book.pdf

would drive change at the “right assembly scale level” and the Multi-Party Engineering methods would enable the change to be executed in the AAE in as small and incremental fashion as possible.

Accepting the new challenges of providing, trading, and assembling components requires a significant shift in perspective among acquisition and security professionals. By contrast, end users of the operational networks have long been forced to make changes to delivered IT systems in the field. End users who receive assembled IT capabilities in which they can substitute components in an orderly fashion when needed would likely find that a natural activity once they receive proper training.

Table 2 summarizes some of the obvious shifts in program perspective regarding acquisition. The perspectives are phrased in terms of “owning,” “depending,” and “trusting,” since the latter represents the most significant change. The table captures a snapshot in time, because both the shifts and our understanding of them will grow with experience.

Table 2. Shift in Perspective

Topic	Standalone System Perspective	Assembled Capability Perspective
Infrastructure	<ul style="list-style-type: none"> • Own all infrastructure except for network (sometimes) and power (usually). 	<ul style="list-style-type: none"> • Trust and depend on someone else’s shared infrastructure.
Hardware/software	<ul style="list-style-type: none"> • Own/operate my own production hardware. • Run my software on my hardware. • Manage my software. 	<ul style="list-style-type: none"> • Trust and depend on someone else’s hardware. • Trust and depend someone else to manage my software.
Data	<ul style="list-style-type: none"> • Own all the data that resides on my systems. • Everyone else must pay me and make special requests to get any data I own. • Assign and control meaning for the data I own. 	<ul style="list-style-type: none"> • Am a steward of data. • The community decides what data means, and which data is useful. • Advertise and provide access to my data to everyone that is authorized. • Will promptly fix problems with data for which I am the steward.
Mission functionality	<ul style="list-style-type: none"> • Mission functionality is not my sole focus. • In parallel also have to deliver infrastructure 	<ul style="list-style-type: none"> • Mission functionality is my sole focus (if I provide mission components). • Shared infrastructure is my sole focus (if I provide shared infrastructure). • Data is my sole focus (if I provide data exposure components).
Program Office	<ul style="list-style-type: none"> • Own the budget, and the bigger the better from a career growth potential. • Offload most/all risk to the contractor. • My success depends only on me. 	<ul style="list-style-type: none"> • Budget fluctuates depending on validated needs of the community. • One of many team players. • My success depends on many people.

Recommendations

The ongoing efforts described above, observed maturity levels, and current challenges lead us to offer several initial recommendations. We make these recommendations knowing that some stakeholders within DoD, industry, academia, Federally Funded Research and Development Centers) National Labs, etc., are starting to transition from delivering standalone systems to delivering assembled IT capabilities. Thus, stakeholders should recognize that they must (a) accept a new set of component, market, and assembly challenges, and (b) transform themselves to meet these challenges.

To enable change for the security professionals and the developers who must support them we recommend the following:

1. Create a nominal component lifecycle. The high-level lifecycle would foster agreement among stakeholders across direct efforts as to the generic and repeatable nature of cybersecurity actions. Below the high-level lifecycle would be two levels of specialization: one for the type of software component technology and intended component use, and the other per organization. With regard to software, each type of component would likely result from specialized processes particular for to that technology. The high-level process would identify roles and responsibilities pertinent to development, testing, and vetting procedures and documentation, especially roles and responsibilities concerning with regard to assessing a component via automated and manual means. However, different organizations might use different names for specific personnel billets, although they perform similar high-level functions. Thus, the DoD should establish common terminology to ensure that all parties to agreements have the same understanding of responsibilities.
2. Create agreed 8510.01 product-level Security Assessment Reports (SARs) for each component type (in contrast to current 8510.01 SAR templates, which are oriented toward system development). The component lifecycle Shared Agreements described above could be used to create initial product-level SARs to inform future RMF implementation guidance. Organizations should also create trusted means to store and transmit product-level SARs (materiel)

Community and enterprise policy and guidance bodies should consider the following recommendations to broaden the adoption of components, markets, and assembled IT capabilities:

1. Create a nominal component adoption “organizational readiness” scale to ensure that organizations become aware of the change of perspectives, as well as pertinent challenges to meet. The readiness scale would cover both organizations and the individual personnel categories within those organizations, and outline the steps they should undertake to adopt components, markets, and assembled IT capabilities. We anticipate that the DoD would need to measure readiness to perform various technical activities (e.g., vetting components), as well as readiness to engage in cooperative activities such as governance, active participation in communities of practice, etc. This scale could also address the shortfall in ability to measure maturity, as noted earlier in the paper

2. Create an enterprise roadmap for enabling adoption of components and assembling capabilities. The enterprise roadmap would include high-level goals for the enterprise, such as that expressed by JIE. In addition, since every mission is unique, and the various COCOMs and Services that participate in the AAE have differing needs as well, the enterprise roadmap must be guided by feedback from end users and direct efforts, analogous to the recommendation for cyber security. In addition to working with direct efforts, the DoD should ensure the rest of the enterprise also identifies challenges and creates strategies to meet these challenges. Candidate roadmap topics include requirements, business model, funding, change management and dependency strategies, testing, training, and the help desk.

Conclusion: 2014 Is a “Tipping Point”

The year 2014 can be a tipping point for using Multi-Party Engineering to adopt approaches based on components, markets, and assembled IT capabilities. The DoD can now connect data, and has almost reached the point of being able to assemble its overall response to match the need posed by a given event, provide feedback to shape the capability assembly at multiple scales, and capture lessons learned and drive component and IT assembly changes for future events. Components and assemblies themselves yield benefits in terms of IT efficiencies and enable greater focus on mission functionality. Additional synergy can emerge from parallel assembly approaches for populating federated mission networks in C/JTFs, and even assembling coalition forces in response to events. The multi-scale, multi-time nature of the various assemblies may increase mission focus and potential agility, as well as reduce cost. However, to fulfill the vision and achieve the benefits, the DoD must address significant challenges that include cybersecurity reciprocity, business models, federation, community, and infrastructure.

As with all big changes, motivation stems not just from a compelling vision, but from the closing of previously available options. The DoD can no longer afford the present method of delivering standalone systems. The pressures of budgets, time, and sustainment all force the DoD away from its present approaches. As in any transformation, the DoD will need to be selective: to choose which standalone systems to deconstruct in order to harvest its components, which new components to build, and which new capability assemblies to deliver.

The DoD can let the forces act and in effect make default decisions, or it can seize the initiative and incrementally grow AAEs based on usage, via a number of direct, community, and enterprise efforts. Such ecosystems would feature many governed independent actors such as the providers of components, assembled capabilities, and shared infrastructure, partner nations, and event commanders. The component and assembled IT capabilities would be offered in markets, ready to be assembled at multiple scales for the next event.

Afterword

There are many activities just touched on in this paper which should be pursued in order to assure rigorous and enduring adoption of the Agile and Adaptive Ecosystem. For example we will need a

repository or catalog of Shared Agreements in all their forms, across the enterprise. This will help understanding a variety of aspects about components in markets, such as cybersecurity, product license/usage, compatible mission threads, etc. Perhaps over time, a living catalog of the Shared Agreements could help enable the Agile and Adaptive Ecosystem to achieve a TRL9+ (Technical Readiness Level).

It is important to note that mutual awareness of the activities across all the efforts happens informally via a variety of community and enterprise communities of practice, Joint C2 and DI2E community forums, and interaction with specific efforts. Thus, our knowledge is imperfect, and by definition always out of date, because these forums are periodic, and not yet strongly coordinated. If the reader has additional examples of efforts and maturity in the DoD they would like to share, please contact the authors.

ICCRTS 2014

Agile and Adaptive IT Ecosystem, Results, Outlook , and Recommendations (paper 011, track 4)

Harvey Reed (MITRE)

John "Nano" Nankervis (Joint Staff J6)

LtCol Jordon Cochran (OUSD / AT&L)




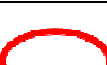

Rajeev Parekh, US BICES Chief Engineer, (MITRE)

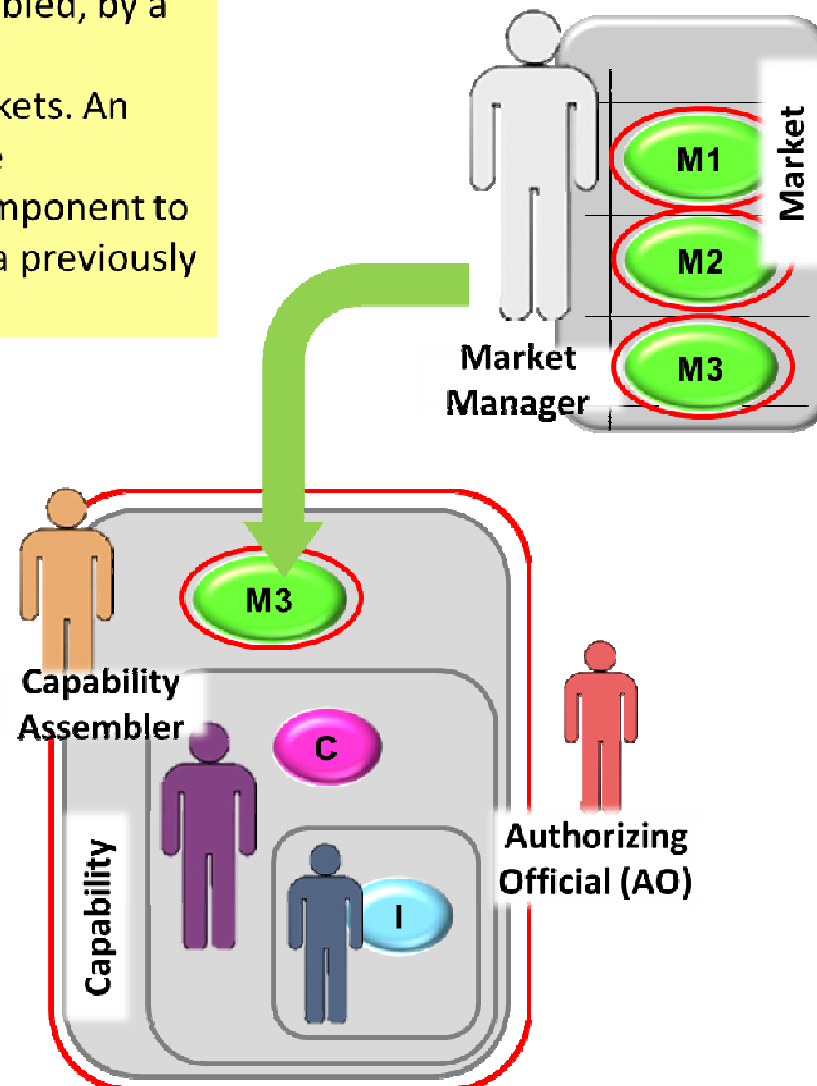
Fred Stein, Col. U.S. Army (ret) (MITRE)

Vision: Assemble IT Capabilities

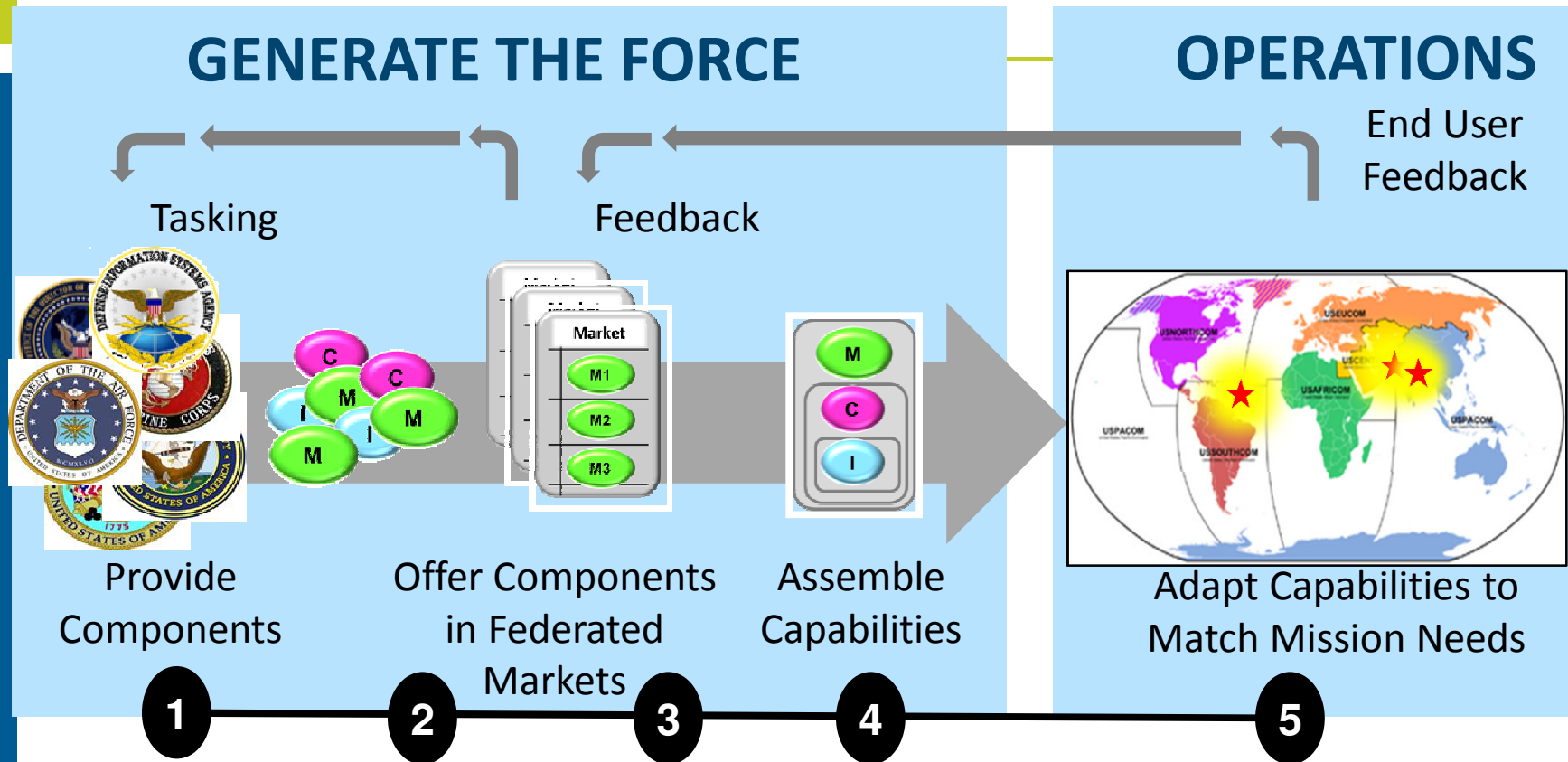
IT Capabilities can be assembled, by a Capability Assembler, from components offered in Markets. An Authorizing Official uses the assessment of a mission component to authorize it for inclusion in a previously accredited boundary.

LEGEND

	Mission Component e.g. WebApp
	Core Component e.g. Server
	Infrastructure Component e.g. Cloud
	Assessment of mission component
	Accreditation boundary for assembled capability



Agile and Adaptive Ecosystem



Multi-Party Engineering grows the AAE:

1. Provide components
2. Offer components in markets
3. Certify components to shared agreements
4. Use Components to assemble capabilities
5. Solicit and respond to feedback from users

Results 1 of 2

Type of Effort	Description	Activity Level	Examples
IT Capability	Use a variety of mission and core infrastructure components to assemble an IT capability	Significant	<ul style="list-style-type: none"> Joint Logistics Enterprise Data Sharing (JLEDS), complete C-130 Electronic Flight Bag, in progress
New components; components harvested by deconstructing legacy components	Employ methods that range from community-wide data calls to identify new and/or potentially reusable services, to harvesting as a result of legacy deconstruction. Some components are traded across joint and/or family of systems organization boundaries.	Significant	<ul style="list-style-type: none"> Global Command and Control System – Joint (GCCS-J) and ACF (Agile Client Framework), complete Defense Intelligence Information Environment-Framework (DI2E-F), in progress Theater Battle Management Core System-Unit Level (TBMCS-UL), Command and Control Information Systems / Command and Control Air Operations Suite (C2IS/AOS), in progress
Hosting, platform	Engage in efforts ranging from classic hosting to cloud migration	Significant	<ul style="list-style-type: none"> Global Combat Support System – Air Force (GCSS-AF), complete Federal Risk and Authorization Management Program (FEDRAMP), complete CIO Cloud Strategy, complete Defense Information Systems Agency (DISA) Cloud Broker, in progress

Results 2 of 2

• Type of Effort	Description	Activity Level	Examples
• Mobile	Effort to use smartphones and other mobile devices	Very significant	<ul style="list-style-type: none">• CIO Mobility Strategy, complete• National Geospatial-Intelligence Agency (NGA) Geospatial Intelligence (GEOINT) App Store, in progress• DoD Mobility, in progress• General Services Administration (GSA) Managed Mobility, in progress
• Markets and federation	Broad need to trade components across Title 10 and other organization boundaries.	Emerging	<ul style="list-style-type: none">• Combatant Commands (COCOMs) and Services, in progress
• Component cybersecurity reciprocity	Ability to trade components across designated Authorizing Official (AO) boundaries	Emerging	<ul style="list-style-type: none">• DoD Widget Working Group (WG), in progress

Maturity Scale (1 of 2)

Based on Multi-Party Engineering Tenets

Multi-Party Engineering Tenet	Example Activity
1. Provide Components	Both the Agile Client and Ozone Web Framework marketplaces demonstrate that program offices can build and/or acquire a component for their own use.
2. Certify components to Shared Agreements	Ongoing activities within DI2E-F aim to understand what it means for the community to agree (certify) that a service (component) is suitable for reuse, at least within the certifying community. Activities within DISA and NSA are seeking approaches to standardize vetting of mobile apps.
3. Offer Components in markets	Some markets are relatively mature, such as the NGA GEOINT app store; other markets are only beginning to develop. In some tactical cases, the DoD does not use markets in order to prevent changes to component configuration in the field.

Maturity Scale (2 of 2)

Based on Multi-Party Engineering Tenets

Multi-Party Engineering Tenet	Example Activity
4. Use components to assemble capabilities	<ul style="list-style-type: none"> • GCSS-AF presents a very mature example of full-service hosting • Some early examples of dedicated function-assembled capabilities (e.g., JLEDS) are appearing. • For dashboards, a server hosts several instances of web apps that are visualized as tiles in a browser for the purpose of organizing data for the user • Rapid assembly of mobile apps is gaining popularity. The DoD CIO and DISA are establishing strategies.
5. Solicit and respond to feedback from users	<p>MPE grows an AAE over time, at many scale levels by using feedback from end users as input to the requirements and governance of markets. No central planning takes place; however, developers receive feedback from users through local and community centers of federated governance. Some feedback loops are emerging at the direct, community, and enterprise levels. The feedback loops are ultimately the most important feature of the ecosystem</p>

Challenges

- 1. Cybersecurity reciprocity for mission-oriented software-only components.**
- 2. Create a business model(s) that enables repeatable and rapid acquisition of components and assembled capabilities**
- 3. Market federation to enable trading of components via markets across Title 10 and other boundaries.**
- 4. Build a community(s) that facilitates highly matrixed sharing of practices and case studies across direct, community, and enterprise efforts.**
- 5. Create and maintain a baseline of infrastructure and platforms that host various types of components.**

Outlook

■ JIE

- Currently the bulk of direct, community, and enterprise efforts using Multi-Party Engineering are developed, deployed, and operated in the context of the U.S. and regional and mobile networks that are evolving to the JIE.

■ Mission Partner Environment

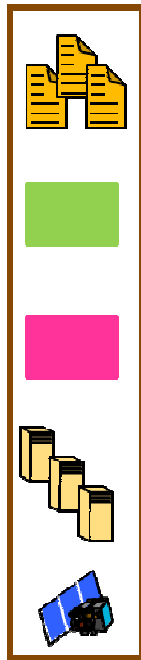
1. The components, markets, and assembled IT capabilities are starting to add value in the JIE. The value will be fully realized once DoD programs can deploy assembled capabilities to operational networks, including the Mission Partner Environment.
2. The agreement structure required for assembling IT capabilities resembles the agreement structure in Mission Partner Environment

Changing Perspectives

Today:

Each system requires
One dedicated program office

Acquisition/Accreditation Boundary

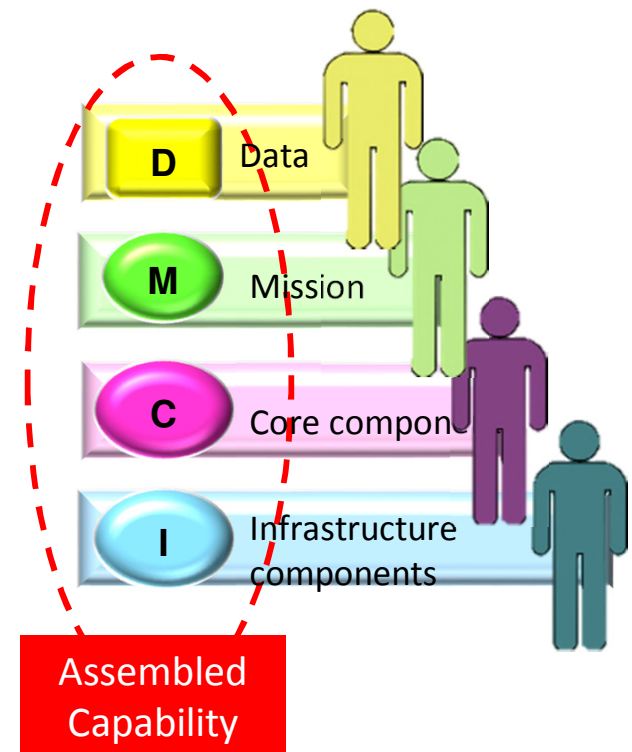


Mission
Information
Mission
Functionality
Core /
Middleware
Computing
Network



Tomorrow:

Each assembled capability requires
Multiple program offices



Competencies: Provide components, Assemble capabilities, Manage dependencies

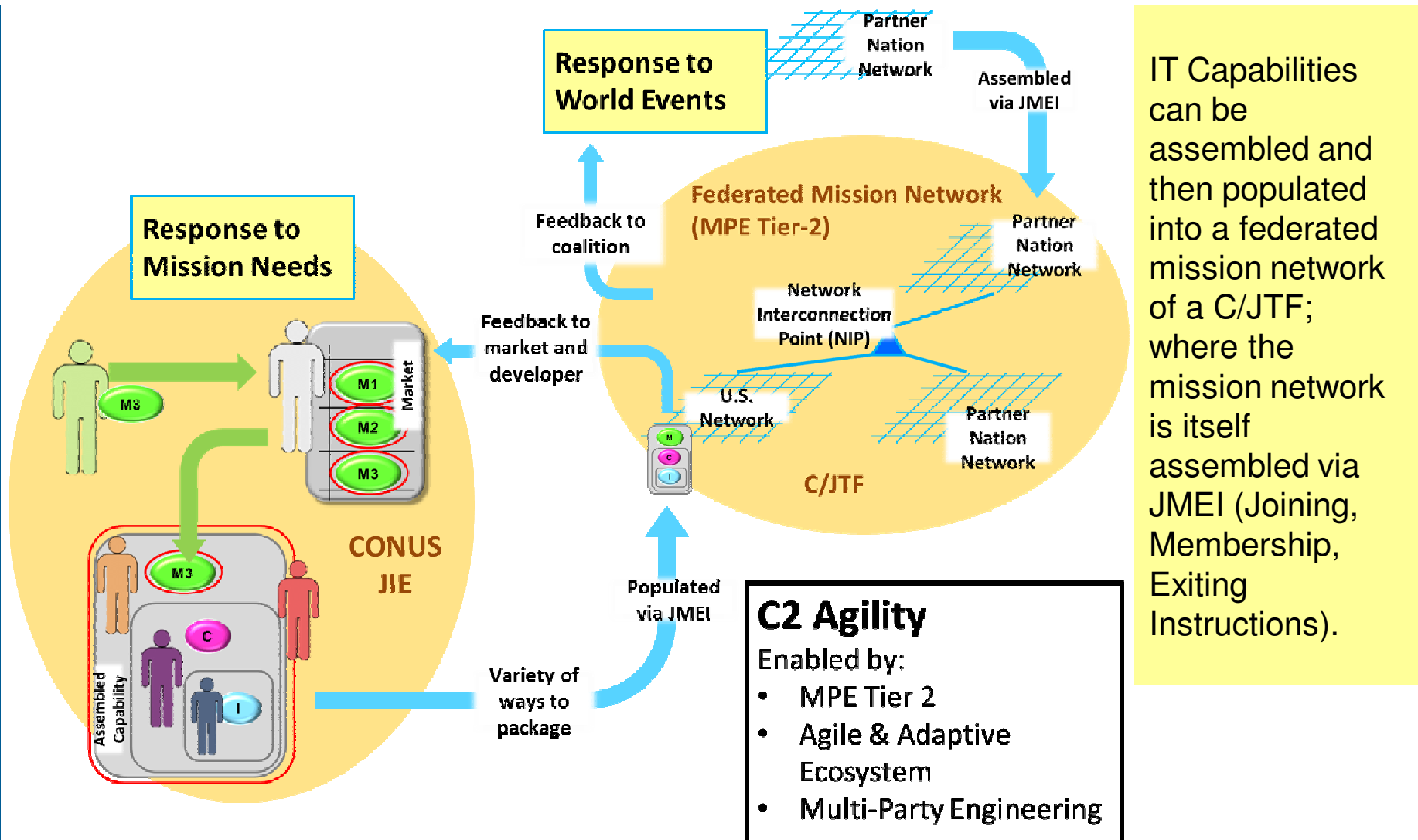
Recommendations

- 1. Create a nominal component lifecycle:**
 - Foster agreement among stakeholders across direct efforts as to the generic and repeatable nature of cybersecurity actions.
- 2. Create agreed 8510.01 product-level Security Assessment Reports (SARs) for each component type:**
 - This is in contrast to current 8510.01 SAR templates, which are oriented toward system development.
- 3. Create a nominal component adoption “organizational readiness” scale:**
 - Ensure organizations are aware of the change of perspectives, and challenges to meet.
- 4. Create an enterprise roadmap for enabling adoption of components and assembling capabilities:**
 - High-level goals for the enterprise, such as that expressed by JIE.
 - Must be guided by feedback from end users and direct efforts.

Conclusion: 2014 is a “Tipping Point”

- **Increasing need**
 - World events happen at an accelerating pace
 - Adversaries increasingly agile
- **Compelling Vision**
 - Commercial industry creating component technology at an accelerating pace
 - Practices starting to come into focus, i.e. Multi-Party Engineering which grows an Agile and Adaptive Ecosystem
- **Closing of Current Options**
 - Declining budgets
 - Very few “new starts” for big systems
- **Increasing Momentum**
 - DoD starting to adopt and understand necessary changes
 - Industry organizing to understand, partner and help drive change, i.e. Industry Advisory Group (part of AFEI/NDIA)

Vision: Assemble IT, Assemble C/JTF



Team

■ Authors

- Harvey Reed, Multi-Party Engineering, MITRE, hreed@mitre.org
- John Nankervis, Mission Partner Environment, CIV Joint Staff J6, john.t.nankervis.civ@mail.mil
- LtCol Jordon Cochran (USAF), OUSD(AT&L), jordon.t.cochran.mil@mail.mil
- Rajeev Parekh, US BICES Chief Engineer, MITRE, rparekh@mitre.org
- Fred Stein, Col. U.S. Army (ret), Network Centric Warfare, MITRE, fstein@mitre.org

■ POC

- Harvey Reed, hreed@mitre.org

■ Contributing

- Robert (Pat) Benito, Multi-Party Engineering, MITRE, rbenito@mitre.org
- Chris Magrin, DISA PEO-C2C Chief Engineer, MITRE, cmagrin@mitre.org
- Diane Hanf, Multi-Party Engineering, MITRE, ghanf@mitre.org
- Michelle Casagni, Multi-Party Engineering, MITRE, mcasagni@mitre.org

Multi-Party Engineering is emerging from Community and Direct Efforts

